Policy Name:	**Ingevity Guest Network Acceptable Use Policy**
Maintained by:	Information Security
Policy Scope:	Guest Wireless Network (INGGuest)
Policy Region:	Global
Last Reviewed:	Oct 2023

TABLE OF CONTENTS

1. Introduction

   This document is an addendum to the Ingevity IT Acceptable Use Policy. This policy is administered by Ingevity Information Security and will be reviewed and updated each calendar year (or more frequently as needed) to reflect changes in corporate risk tolerance or the risk environment.

2. Scope

   This policy applies to all Ingevity employees, guests, associates, contractors, or other authorized personnel across all domestic and international business units.

3. Purpose

   This policy defines the acceptable use of Ingevity's guest network (INGGuest) made available by Ingevity for authorized users. Inappropriate use could expose Ingevity to risks including malware infections, disruption of network systems and services, compromise of intellectual property, unauthorized access to personal identifiable information, and litigation. Authorized users shall not use the guest network for unlawful or unauthorized purposes.

4. Policy Enforcement

   Management must make this policy accessible to all employees and guests for awareness and inform them of their responsibilities before granting access. Managers are also in charge of enforcing this policy in their departments. If there's a policy violation, management will raise awareness, offer guidance, and take corrective action when needed. Ingevity can revoke access for those who breach this policy.

5. Consent to Monitoring

   Ingevity may monitor, record, log, review, and disclose all information stored or transmitted by an Ingevity owned asset or on the Ingevity corporate network, including the guest network, at any time without notice for purposes of legal investigations, examining suspicious activity, or for incident response. All employees and guests consent to this monitoring, logging, review, and disclosure. Ingevity does so while acting within the laws of each state and/or country. Executing any additional form of network monitoring with the intent to intercept or view data, unless authorized and approved by Information Security, Legal, and Human Resources, is prohibited.

6. Personal Devices

   Personal or non Ingevity owned devices are allowed to connect via wireless to the guest network (INGGuest) for internet access. Personal wireless access points may not be physically connected (tethered) to any part of the Ingevity physical network or company asset without approval in advance by Information Security.

   The use of a personal mobile device as an access point for an Ingevity laptop is permitted.

7. Internet Usage

   Employees and guests are prohibited from using network monitoring, network penetration, vulnerability scanning, or network discovery tools while accessing the guest network. Additionally, sending email considered to be or containing "SPAM", "chain letters", "ponzi" or other "pyramid" schemes, service advertisements, or harassment of any type while accessing the guest network is prohibited. Ingevity filters access to Internet websites that present risk, are deemed inappropriate, or have been determined unacceptable for the business environment. The following categories of websites are examples of filtered access.

   - Adult/Sexually Explicit Material
   - Advertisements & Pop-Ups
   - Extremism
   - Gambling
   - Games
   - Hacking
   - Illegal Drugs
   - Nudity
   - Shareware and Freeware
   - SPAM, Phishing, and Fraud

- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate

Ingevity leadership and Information Security periodically reviews and recommends changes to the established web filtering rules based on industry standard practices and corporate policies.

8. Local, Provincial/State, Federal, and International Law

   Under no circumstance is an employee or guest of Ingevity authorized to engage in any activity that is illegal under local, provincial/state, federal, or international law while using Ingevity's guest network.